Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
  ATO - Authorization to Operate
  CAC - Common Access Card
  FISMA - Federal Information Security Management Act
  ISA - Information Sharing Agreement
  HHS - Department of Health and Human Services
  MOU - Memorandum of Understanding
  NARA - National Archives and Record Administration
  OMB - Office of Management and Budget
  PIA - Privacy Impact Assessment
  PII - Personally Identifiable Information
  POC - Point of Contact
  PTA - Privacy Threshold Assessment
  SORN - System of Records Notice
  SSN - Social Security Number
  URL - Uniform Resource Locator

Does this need to migrate to a Sub-Component?:

Consolidated Parent Component

Component Name
No Records Found

General Information

PIA Name:	CDC - TAC - QTR3 - 2023 - CDC6788460	**PIA ID:**	6788460
Name of Component:	Technical Assistance Center	**Name of ATO Boundary:**	Technical Assistance Center

Migrated Sub-Component PIA

PIA Name
No Records Found

Sub-Component

Software Name
No Records Found

Original Related PIA ID

PIA Name
No Records Found

Overall Status:	✅	**PIA Queue:**	
Submitter:	COLLINS, LaQuawn PATEL, Anusha	**# Days Open:**	136
Submission Status:	Re-Submitted	**Submit Date:**	9/29/2023
Next Assessment Date:	11/16/2026	**Expiration Date:**	11/16/2026
Office:	DDNID	**OpDiv:**	CDC
Security Categorization:	Low		
Legacy PIA ID:		**Make PIA available to Public?:**	Yes
1:	Identify the Enterprise Performance Lifecycle Phase of the system		Operations and Maintenance
2:	Is this a FISMA-Reportable system?		Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?		Yes
4:	ATO Date or Planned ATO Date		9/7/2023

Privacy Threshold Analysis (PTA)

PTA Name
CDC - TAC - QTR2 - 2023 - CDC6757254

History Log:	**View History Log**

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The system name was changed from Technical Assistance Hub (TAH) to Technical Assistance Center (TAC).

PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	The purpose of this system is to support a Technical Assistance Center (TAC) that delivers comprehensive technical assistance and training to support the successful implementation and evaluation of surveillance and prevention activities for the recipients of Division of Overdose Prevention (DOP) programs, such as the Overdose Data to Action (OD2A). The DOP Technical Assistance Center (TAC) websites offers a repository of overdose surveillance and prevention resources for both Division of Overdose Prevention (DOP) staff and recipients of Division of Overdose Prevention (DOP) programs. Additionally, the Technical Assistance Center (TAC) website is used to track and monitor the technical assistance that is delivered to Division of Overdose Prevention (DOP) recipients.
PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The system will collect the following data: Basic program information on Overdose Data to Action (OD2A), Overdose Data to Action (OD2A) program participants request for Technical Assistance Center, The administration and execution of the Technical Assistance Center, Events and activities that can be attended by program participants and interested parties, Resources and publications that are curated and disseminated by Overdose Data to Action (OD2A) subject matter experts, and User information for program participants (Username, name, business/organizational email address).
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	Non-HHS User Credentials Username Password Email Address

PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	Technical Assistance Center (TAC) collects data from stakeholders who oversee, implement, and support the program activities under OD2A, including state agency administrators, program staff, local health department staff, and evaluators. Data collection will include the TA utility, preferences, needs, and interests for the optimal delivery of TA content across a diverse group of stakeholders who are directly involved in building or sustaining opioid surveillance and prevention program activities.

The Overdose Data to Action (OD2A) Technical Assistance Center (TAC) evaluation surveys involves the use of web-based data collection methods. The website does use cookies, and access to the web-based questionnaire will use a link to an anonymous survey. The data will be used in the administering of the Technical Assistance. Monthly reports will be created from the analytics within the system, and it will be shared with the Program team and CDC program officers and managers.

PII Information (Username, name, Business/organizational email address) is collected solely for the purposes of providing password-protected access to the OD2A-TAC website, facilitating internal communication among OD2A-TAC website users, sending system notifications, follow-up, and sending communications and announcements from OD2A-TAC, and monitoring and tracking reach and use so to meet users' needs.

No data is extracted from this system and fed into another system. |
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes

PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The Technical Assistance (TAC) publicly available website is used for user login activities (login and password reset) and contact information for the Division of Overdose Prevention for those seeking help or access to the system. Only authorized users are allowed to access the non-publicly available portion of Technical Assistance Center (TAC) system. The purpose of TAC is to deliver comprehensive technical assistance and training to support the successful implementation and evaluation of surveillance and prevention activities for the recipients of Division of Overdose Prevention (DOP) programs, such as the Overdose Data to Action (OD2A). The Division of Overdose Prevention (DOP) TAC websites offers a repository of overdose surveillance and prevention resources for both Division of Overdose Prevention (DOP) staff and recipients of Division of Overdose Prevention (DOP) programs. Additionally, the TAC website is used to track and monitor the technical assistance that is delivered to DOP recipients. Recipients and program participants must request for site access with the CDC. Once their application for access has been reviewed and approved, a user profile is created for the user and they are sent a welcoming email to their email address. Once they have access to the website, they can log into the site via a browser and view resources, event announcements, other members. Program recipients can request technical assistance. This assistance is performed outside of the system, but the interactions are recorded in a Technical Assistance Assignment and then generate a Technical Assistance report that summarizes the interaction and outcomes.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	Yes
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes
PTA - 12:	Does the website use web measurement and customization technology?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	No
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	

PTA - 17:	Does the mobile application contain links to non-federal government website external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Employment Status User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	The PII Information is used for user registration, login and contact and follow-up.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	N/A
PIA - 6:	Describe the function of the SSN and/or Taxpayer ID.	N/A
PIA - 6A:	Cite the legal authority to use the SSN.	N/A
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Public Health Service Act, Section 301, "Research and Investigation" (42 U.S.C. 241)
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	

PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains
		In-person
		Email
		Government Sources
		Other HHS OPDIV
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	OMB # 0920-1355.
PIA - 10B:	Identify the OMB information collection approval number expiration date.	11/30/2024
PIA - 10C:	Explain why an OMB information collection approval number is not required.	The OMB # is required.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	There is no method to opt out of the collection of the PII for this systems since the PII collected is name, email address, and employment status is required in order to communicate with the site users. We could not communicate or authenticate the users without the PII requested.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	The participants are contacted via email to notify and obtain consent when major changes occur.

PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	User PII is limited to name, email, jurisdiction, and role – all of which are intended to be shared within the system with other users, via a member directory. Internal sharing of this information facilitates connections and communication among OD2A recipients, who are eager to learn from and support one another. The notice on the member directory records reminds users "Personally identifiable information (e.g., name, email address) is provided solely for the purposes of internal communication among OD2A Technical Assistance Center (TAC) website users and for system notifications.". Users also have access to their own account profile, which they can update or correct at any time, to fix any inaccurate PII. Users can contact overdosedata2action@cdc.gov with concerns about the use of their personal information.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	The system automatically prompts users (via email) every 60 days to update their password and review their profile information. This encourages self-maintenance of PII. New requests for system access are reviewed to ensure that only agency email addresses are used and to check for correct role selection. They are also reviewed and approved by DOP before being added to the system. This process takes place on a rolling basis to ensure new users are added to the system in a timely manner. Contractor Administrators and Developers may also access user profiles when needed – for example to delete them if DOP leadership requests this (for a recipient who had retired or resigned, for example).
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: The users have access to PII for collaboration and or editing. Administrators: Indirect contractors add, edit, remove; PII to ensure integrity, accuracy and relevancy of information. Developers: Indirect contractors debugging data-related issues. Contractors: Indirect contractors add, edit, remove; PII to ensure integrity, accuracy and relevancy of information.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users' roles are approved by the program management team and they do not have access to PII. The program management team must approve all user role classifications before they are assigned by the site administrator. This ensures only authorized users can have access to the PII.
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	The site will only collect the bare minimum PII in order to register the user on the site and ensure that the user is who they say they are. Furthermore, role-based access control are in place to ensure the concept of "least privilege" is implemented. Job function determines the level of access and users are assigned only those rights necessary to fulfill responsibilities for approved roles and system-level audit controls to safeguard and audit use.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.	All staff are required to take annual training in cybersecurity, security awareness, and privacy training. This training has been reviewed and is in accordance with the CDC requirements.
PIA - 22:	Describe training system users receive (above and beyond general security and privacy awareness training).	Training for administrators and developers is tailored to the TAC information system and their roles.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	Records are retained and disposed of in accordance with the CDC Records Control Schedule (N1-442-09-1) and in accordance with contractual agreement. Record copy of study reports are maintained in the agency from two to three years in accordance with retention schedules. Source documents for computers are disposed of when they are no longer needed by program officials. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records are retained for 20 years; for longer periods if further study is needed.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	**Administrative** The administrative security controls employed include adhering to department, policies and procedures around security and privacy; and annual awareness training for all users holding accounts for the system. **Technical** The technical controls are shared between the system and Acquia's Amazon Web Service (AWS) platform. The system provides controls such as multi- factor authentication for all users to include Personal Identity Verification (PIV) login capability and role-based system access to control the amount of PII available to a user; 2 rounds of two-factor authentication for each individual accessing a data

center floor. Acquia's AWS provides infrastructure controls such as secure network access points.

Physical

Physical access authorizations at entry/exit points to the facility where the information system resides by verifying individual access authorizations before granting access to the facility; and controlling ingress/egress to the facility Cloud Service Provider (Acquia hosting is using the Amazon Web Service (AWS) cloud) defined physical access control systems/devices and guards. The organization also maintains physical access audit logs for entry/exit points and provides security safeguards to control access to areas within the facility officially designated as publicly accessible and escorts visitors and monitors visitor activity in all circumstances within restricted access area where the information system resides; secures keys, combinations, and other physical access devices; inventories of organization-defined physical access devices at least annually. Following are the AWS Data Center Access controls:

EMPLOYEE DATA CENTER ACCESS

AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

THIRD-PARTY DATA CENTER ACCESS

Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

AWS GOVCLOUD DATA CENTER ACCESS

Physical access to data centers in AWS GovCloud (US) is restricted to employees who have been validated as being US citizens.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	10/3/2023
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: October 3, 2023 Appears that acronym at issue was removed in PIA 24.	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	JWO Signature.docx
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	10/5/2023
		SOP Days Open:	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	10/6/2023
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski This PIA is ready for SAOP review and approval. There was only one comment but it is for the next iteration of the PTA: On the next iteration of the PTA: PTA-5 and PTA-6: please include "Employment Status" as one of the PII data element collected.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	
SAOP Comments:	On behalf of Bridget Guenther In the next iteration of the PIA, please address the comments regarding PTA-5 and PTA-6. Please also confirm the type of web customization and measurement technology used (i.e., cookie or other technology) to resolve the inconsistency in the responses.	**SAOP Review Date:**	11/17/2023
		SAOP Days Open:	42

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	MOSIOS, Joshua	8/7/2023	Employment status was previously listed as a data element collected by this system. Is this still true? If so, please include here. If not, please explain in the comment section (the yellow note pad on the right of the screen). If the latter, please address the following questions: when that data was removed? Why was the data removed? How was the data removed? Was the data destroyed? If so, how was it destroyed? If not, where is the data now? How is the data being secured? Who is protecting the data?	
PIA - 24	MOSIOS, Joshua	8/7/2023	Physical controls cannot be provided by a technical platform. Please elaborate on the physical control owners and their processes.	
PIA - 24	OSHODI, Jarell	9/18/2023	Define CSP.	
PIA - 1	Data Feed Service, Sync2PIAForm	10/6/2023	On the next iteration of the PTA: PTA-5 and PTA-6: please include "Employment Status" as one of the PII data element collected.	